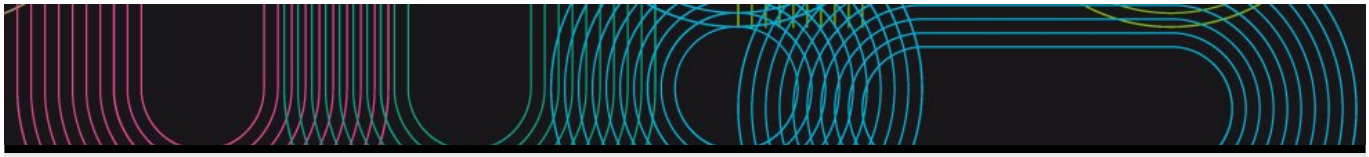

DATOS IDENTIFICATIVOS				
Seguridad en sistemas de información				
Asignatura	Seguridad en sistemas de información			
Código	P52M182V01207			
Titulacion	Master Universitario en Dirección TIC para la defensa			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	4	OP	1	2c
Lengua Impartición	Castellano			
Departamento				
Coordinador/a	Fernández Gavilanes, Milagros			
Profesorado	Fernández Gavilanes, Milagros Vales Alonso, Javier			
Correo-e	mfgavilanes@cud.uvigo.es			
Web	http://campus.defensa.gob.es | https://moovi.uvigo.gal			
Descripción general	La asignatura de Seguridad en sistemas de información mostrará las técnicas, protocolos y arquitecturas relacionadas con la seguridad que existen en los distintos niveles de implementación de un sistema de información moderno, con un énfasis particular en la parte de las comunicaciones. La asignatura se enfocará a la exposición clara de estos problemas, y a la resolución práctica de los mismos mediante casos de estudio prácticos.			

Resultados de Formación y Aprendizaje	
Código	
A6	CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
A7	CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
A8	CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
A9	CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
A10	CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
B1	CG1 - Poseer conocimientos avanzados y altamente especializados y demostrar una comprensión detallada y fundamentada de los aspectos teóricos y prácticos tratados en las diferentes áreas de estudio.
B2	CG2 - Integrar y aplicar los conocimientos adquiridos, y poseer capacidad de resolución de problemas en entornos nuevos o definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar relacionados con su ámbito de estudio.
B7	CG7 - Valorar la importancia de los aspectos de seguridad en la gestión de sistemas e información, identificando necesidades de seguridad, analizando posibles amenazas y riesgos y contribuyendo a la definición y evaluación de criterios y políticas de seguridad.
C18	CISTI4 - Definir, analizar e implantar los mecanismos de seguridad durante todo el ciclo de vida de los sistemas de información.
D4	CT4 - Capacidad de comunicación oral y escrita de conocimientos.
D6	CT6 - Manejar apropiadamente recursos de información.

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje
RA1. Conocer las amenazas y vulnerabilidades inherentes al desarrollo de software mostrando cómo éste puede hacerse más seguro	A6 A7 A8 A9 A10 B1 B2 B7 C18
RA2. Describir los problemas, amenazas y soluciones empleadas en los distintos niveles de un sistema/servicio de comunicaciones	A6 A7 A8 A9 A10 B1 B2 B7 C18
RA3. Describir las bases técnicas modernas de la criptografía en los que se basan los sistemas de clave simétrica y de clave pública	A6 A7 A8 A9 A10 B1 B2 B7 C18
RA4. Estudiar los sistemas de infraestructura de clave pública, recogiendo en detalle cómo se abordará la creación, mantenimiento, distribución, uso, almacenaje y revocación de certificados digitales	A6 A7 A8 A9 A10 B1 B2 B7 C18
RA5. Describir nuevas aplicaciones y tendencias en el ámbito de la seguridad en los sistemas de información	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4 D6

Contenidos	
Tema	
Tema 1. Introducción a la seguridad en sistemas de información.	- Introducción a los Centros de Datos. - Estructura habitual - Administración de Centros e Proceso de Datos
Tema 2. Seguridad en el desarrollo de software.	- sSDLC - Vulnerabilidades - Contramedidas
Tema 3. Cifrado de clave simétrica.	- Principios matemáticos - Codificadores de bloque (DES, Triple-DES, AES) - Codificadores de flujo (RC4)
Tema 4. Criptografía de clave pública.	- Motivación - Principios matemáticos - Diffie-Hellman - RSA - Criptografía de curvas elípticas (ECC)

Tema 5. Firmas digitales.	- Sistemas de MAC y Hash - MD5 - SHA - HMAC
Tema 6. Sistemas de distribución de claves y autenticación.	- Introducción - Kerberos - X509 - Infraestructura de clave pública (PKI).
Tema 7. Seguridad en transporte y web.	- Motivación - SSL - TLS - SSH
Tema 8. Seguridad en redes.	- IPSec - Firewalls - VPNs - Cloud systems
Tema 9. Tendencias en el uso de sistemas de seguridad.	- Blockchain - Deep web - Anonimización - Criptomonedas - Criptografía de Prueba de conocimiento cero - Cifrado negable - Criptografía de caja blanca - Compartición de secretos - Esteganografía - Criptografía cuántica - Voto electrónico

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Resolución de problemas de forma autónoma	0	9	9
Estudio previo	0	52	52
Lección magistral	8	8	16
Resolución de problemas	3	3	6
Prácticas con apoyo de las TIC	4	0	4
Seminario	4	0	4
Autoevaluación	0	4	4
Presentación	4	0	4
Examen de preguntas de desarrollo	1	0	1

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción
Resolución de problemas de forma autónoma	Actividad en la que el alumnado analiza y resuelve problemas y/o ejercicios relacionados con la materia de forma autónoma.
Estudio previo	Búsqueda, lectura, trabajo de documentación y/o realización de forma autónoma de cualquier otra actividad que el alumno/a considere necesaria para permitirle la adquisición de conocimientos y habilidades relacionadas con la materia. Se suele llevar a cabo con anterioridad a las clases, prácticas de laboratorio y/o pruebas de evaluación.
Lección magistral	Exposición por parte de un profesor/a de los contenidos de la materia objeto de estudio, bases teóricas y/o directrices de un trabajo o ejercicio que el/la estudiante tiene de desarrollar.
Resolución de problemas	Actividad en la que se formulan problemas y/o ejercicios relacionados con la materia. El alumno/a debe desarrollar las soluciones adecuadas y correctas mediante la ejercitación de rutinas, aplicación de fórmulas o algoritmos, la aplicación de procedimientos de transformación de la información disponible y la interpretación de los resultados.
Prácticas con apoyo de las TIC	Actividades de aplicación de los conocimientos en un contexto determinado y de adquisición de habilidades básicas y procedimentales en relación con la materia, a través del uso de las TIC.
Seminario	Actividad enfocada al trabajo sobre un tema específico, que permite ahondar o complementar en los contenidos de la materia.

Atención personalizada

Metodologías	Descripción

Lección magistral	Dado el carácter semipresencial del curso, distinguiremos dos casos: (1) Atención en la fase a distancia: se llevará a cabo mediante el uso de medios telemáticos. Los alumnos que lo deseen podrán plantear dudas al profesorado en foros o mediante correo electrónico. También podrán concertar tutorías individuales con el profesor, que se desarrollarán mediante videoconferencia. (2) Atención en la fase presencial: si bien sigue siendo posible el uso de mecanismos telemáticos de atención al alumno, durante esta fase se emplearán también mecanismos de tutoría presencial.
Resolución de problemas	Dado el carácter semipresencial del curso, distinguiremos dos casos: (1) Atención en la fase a distancia: se llevará a cabo mediante el uso de medios telemáticos. Los alumnos que lo deseen podrán plantear dudas al profesorado en foros o mediante correo electrónico. También podrán concertar tutorías individuales con el profesor, que se desarrollarán mediante videoconferencia. (2) Atención en la fase presencial: si bien sigue siendo posible el uso de mecanismos telemáticos de atención al alumno, durante esta fase se emplearán también mecanismos de tutoría presencial.
Prácticas con apoyo de las TIC	Dado el carácter semipresencial del curso, distinguiremos dos casos: (1) Atención en la fase a distancia: se llevará a cabo mediante el uso de medios telemáticos. Los alumnos que lo deseen podrán plantear dudas al profesorado en foros o mediante correo electrónico. También podrán concertar tutorías individuales con el profesor, que se desarrollarán mediante videoconferencia. (2) Atención en la fase presencial: si bien sigue siendo posible el uso de mecanismos telemáticos de atención al alumno, durante esta fase se emplearán también mecanismos de tutoría presencial.
Seminario	Dado el carácter semipresencial del curso, distinguiremos dos casos: (1) Atención en la fase a distancia: se llevará a cabo mediante el uso de medios telemáticos. Los alumnos que lo deseen podrán plantear dudas al profesorado en foros o mediante correo electrónico. También podrán concertar tutorías individuales con el profesor, que se desarrollarán mediante videoconferencia. (2) Atención en la fase presencial: si bien sigue siendo posible el uso de mecanismos telemáticos de atención al alumno, durante esta fase se emplearán también mecanismos de tutoría presencial.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Prácticas con apoyo de las TIC	Actividades de aplicación de los conocimientos en un contexto determinado y de adquisición de habilidades básicas y procedimentales en relación con la materia, a través del uso de las TIC. Permiten evaluar los conocimientos y habilidades del alumno/a. Se realizarán cuatro actividades entregables (AE1, AE2, AE3 y AE4). Las tres primeras serán evaluadas durante la fase a distancia: AE1 y AE2 abarcarán el tema 3, mientras que AE3 abarcará el tema 4 de la asignatura. En el caso del entregable AE4 este se realizará durante la fase presencial. Cada entregable puntuará un 10% de la nota final.	40	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4
Autoevaluación	Mecanismo en el que, por medio de una serie de preguntas o actividades, se posibilita que el alumno/a evalúe de manera autónoma su grado de adquisición de conocimientos y habilidades sobre la materia, permitiendo una autorregulación del proceso de aprendizaje personal. Se realizará un cuestionario (AV) que abarcará los temas (del 1 al 8) y que se realizará durante la fase a distancia.	10	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4 D6
Presentación	Exposición por parte del alumnado, de manera individual o en grupo, de un tema relacionado con los contenidos de la materia o de los resultados de un trabajo, ejercicio, proyecto, etc. A través de la presentación se pueden evaluar conocimientos, habilidades y actitudes. Este trabajo de presentación (T) será evaluado durante la fase presencial.	20	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4 D6
Examen de preguntas de desarrollo	Prueba de evaluación que incluye preguntas abiertas y/o ejercicios, sobre un tema. Los alumnos/as deben desarrollar, relacionar, organizar y presentar los conocimientos que tengan sobre la materia en una respuesta argumentada. Se puede utilizar para evaluar conocimientos y habilidades. Se realizará una prueba escrita (PE) al final de la fase presencial, en la que se evaluarán todos los temas y contenidos de la asignatura (incluyendo los contenidos de la fase a distancia y de la presencial).	30	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4

Otros comentarios sobre la Evaluación

Si denominamos MED_CON a la nota media de evaluación continua, que se calcula como:

MED_CON = 0.1*AE1 + 0.1*AE2+ 0.1*AE3 + 0.1*AE4 + 0.1*AV + 0.2*T + 0.3*PE

Será necesario sacar una calificación no inferior al 50% para superar la asignatura.

En caso de evaluación en convocatoria extraordinaria el alumno tendrá la opción de volver a realizar (total o parcialmente) las siguientes actividades de evaluación:

- Actividades de autoevaluación (test)
- Evaluación de entregables (prácticas)
- Presentaciones y/o exposiciones
- Prueba escrita

Mientras que la participación en foros se integrará dentro de las actividades de autoevaluación.

Aquellas actividades que el alumno decida repetir se reevaluarán, perdiendo la nota de la convocatoria anterior. La prueba escrita se realizará online.

COMPROMISO ÉTICO:

Se espera que el alumnado tenga un comportamiento ético adecuado, comprometiéndose a actuar con honestidad. En base al artículo 42.1 del Reglamento sobre la evaluación, la calificación y la calidad de la docencia y del proceso de aprendizaje del estudiantado de la Universidad de Vigo, la utilización de procedimientos fraudulentos en pruebas de evaluación, así como la cooperación en ellos implicará la calificación de cero (suspenso) en el acta de la convocatoria correspondiente, con independencia del valor que sobre la calificación global tuviese la prueba en cuestión y sin perjuicio de las posibles consecuencias de índole disciplinaria que puedan producirse.

En el caso de que exista alguna diferencia entre las guías en gallego/español/inglés relacionada con la evaluación prevalecerá siempre lo indicado en la guía docente en español.

Fuentes de información

Bibliografía Básica

William Stallings, **Network Security Essentials. Applications and Standards**, 5, Prentice Hall, 2013

Joshua Davies, **Implementing SSL/TLS. Using Cryptography and PKI**, Wiley, 2011

Bibliografía Complementaria

Tanenbaum Andrew, Wetherall David, **Computer Networks**, 5, Prentice Hall, 2010

Stuart McClure, Joel Scambray, George Kurtz, **Hacking exposed 7 network security secrets and solution**, 7, McGraw‐Hill, 2012

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Seguridad de la información/P52M182V01106